IN THE CLAIMS

1-14. (cancelled).

15. (previously presented) A computer readable storage medium having an invalidity-monitoring program stored thereon, wherein said invalidity-monitoring program, when executed, monitors invalid data which causes a computer to execute an invalid operation, said invalidity-monitoring program comprising:

first software that acquires input/output data that is input or output over a network that is connected to said computer, or over an externally connected bus that connects said computer with an external device;

second software that identifies ID information from said input/output data for identifying a user;

third software that acquires at least part of user attribute data corresponding to said ID information from a user-information-storage unit that stores attribute information for all users having authorization to use said computer;

fourth software that determines whether said input/output data is invalid data by reference to a determination-rule-storage unit that stores rules for determining whether said input/output data is invalid data; and

fifth software that stops an operation executed by said input/output data when said fourth software determines that said input/output data is invalid data;

wherein

said determination-rule-storage unit stores determination rules that correspond to user attributes; and

said fourth software determines whether said input/output data is invalid data in accordance with said determination rules that correspond to user attributes acquired by said third software.

16. (currently amended) The invalidity-monitoring program of claim 15, further comprising:

sixth software that references said user-information-storage unit and determines whether the user corresponding to said ID information has authorization to use said computer; ~~and~~

~~seventh~~ wherein said fifth software ~~that~~ stops operation by said input/output data when said sixth software determines ~~it is determined in the determination~~

~~of authorization~~ that there is no authorization to use said computer;

wherein said sixth software determines authorization of the user to use said computer before execution of said third and fourth software, and when the sixth software determines that there is no authorization to use said computer, said program causes said computer to not execute at least one of the third and fourth software.

17. (currently amended) The invalidity-monitoring program of claim 15, further comprising:

sixth software that references a profile-storage unit that stores log data related to said input/output data as profiles for each user, and compares input/output data acquired by said first software with a normal operation trend of said user to determine whether operation is unusual; and

wherein said fifth software stops an operation executed by said input/output data also when it is determined by said sixth software that ~~said~~ operation is unusual.

18. (previously presented) The invalidity-monitoring program of claim 15, wherein said fifth software executes a process of interrupting a session when said first software acquires said input/output data from a network.

19. (previously presented) The invalidity-monitoring program of claim 15, wherein said fifth software stops a process executed by a driver when said first software acquires said input/output data from an externally connected bus.

20. (previously presented) A computer readable storage medium having an invalidity-monitoring program stored thereon, wherein said invalidity-monitoring program, when executed, monitors invalid data which causes a computer to execute an invalid operation, said invalidity-monitoring program comprising:

first software that acquires input/output data that is input or output over a network that is connected to said computer, or over an externally connected bus that connects said computer with an external device;

second software that identifies ID information from said input/output data for identifying a user;

third software that acquires at least part of user attribute data corresponding to said ID information from a user-information-storage unit that stores attribute information for all users having authorization to use said computer;

fourth software that determines whether said input/output data is invalid data by reference to a determination-rule-storage unit that stores rules for determining whether said input/output data is invalid data; and

fifth software that notifies a terminal being operated by said user or administrator that an operation being executed by said input/output data is an invalid operation when said fourth software determines whether said input/output data is invalid that said input/output data is invalid data;

wherein

said determination-rule-storage unit stores determination rules that correspond to user attributes; and

said fourth software determines whether said input/output data is invalid data in accordance with said determination rules that correspond to user attributes acquired by said third software.

21. (previously presented) An invalidity-monitoring method for monitoring invalid data, which causes a computer to execute an invalid operation, comprising:

acquiring, by said computer, input/output data that is input or output over a network that is connected to said computer, or over an externally connected bus that connects said computer with an external device;

identifying, by said computer, ID information from said input/output data for identifying a user;

acquiring, by said computer, at least part of attribute data corresponding to said ID information from a user-information-storage unit that stores attribute information for all users having authorization to use said computer;

referencing, by said computer, a determination-rule-storage unit that stores rules for determining whether said input/output data is invalid data;

determining, by said computer, whether said input/output data is invalid data based on said rules; and stopping, by said computer, an operation executed by said input/output data when it is determined that said input/output data is invalid data;

wherein

said determination-rule-storage unit stores determination rules that correspond to user attributes; and

in said determining of whether said input/output data is invalid data, referencing said determination rules that correspond to user attributes acquired in said acquiring of attribute information to determine whether said input/output data is invalid.

22. (previously presented) An invalidity-monitoring method for monitoring invalid data, which causes a computer to execute an invalid operation, comprising:

acquiring, by said computer, input/output data that is input or output over a network that is connected to said computer, or over an externally connected bus that connects said computer with an external device;

identifying, by said computer, ID information from said input/output data for identifying a user;

acquiring, by said computer, at least part of attribute data corresponding to said ID information from a user-information-storage unit that stores attribute information for all users having authorization to use said computer;

referencing, by said computer, a determination-rule-storage unit that stores rules for determining whether said input/output data is invalid data;

determining by said computer whether said input/output data is invalid data based on said rules; and

notifying, by said computer, a terminal being operated by said user or administrator that an operation being executed by said input/output data is an invalid operation when it is determined that said input/output data is invalid data;

wherein

said determination-rule-storage unit stores determination rules that correspond to user attributes; and

in said determining of whether said input/output data is invalid data, referencing said determination rules that correspond to user attributes acquired in said acquiring of attribute information to determine whether said input/output data is invalid.

23. (previously presented) An invalidity-monitoring system for monitoring invalid data, which causes a computer to execute an invalid operation, the system comprising:

a computer having a connection to a network or to an external device;

a data-acquisition mechanism for acquiring input/output data that is input or output over the network that is connected to said computer, or over an externally connected bus that connects said computer with the external device;

an ID-information-identifier for identifying ID information from said input/output data for identifying a user;

a user-information-store for storing attribute information for all users having authorization to use said computer;

an attribute-information-acquisition mechanism for acquiring at least part of the attribute data corresponding to said ID information from said user-information-store;

a determination-rule-store for storing rules for determining whether said input/output data is invalid data;

an invalid-data-determination mechanism for referencing said determination-rule-store, and determining whether said input/output data is invalid data; and

a stoppage mechanism for stopping an operation executed by said input/output data when it is determined by said invalid-data-determination mechanism that said input/output data is invalid data;

wherein

said determination-rule-store stores determination rules that correspond to user attributes; and

said invalid-data-determination mechanism references said determination rules that correspond to attribute information acquired by said attribute-information-acquisition mechanism to determine whether said input/output data is invalid.

24. (previously presented) The invalidity-monitoring system of claim 23 further comprising:

a use-authorization-determination mechanism for referencing said user-information-store and determining whether the user corresponding to said ID information has authorization to use said computer;

wherein

said stoppage mechanism also stops operation executed by said input/output data when it is determined by said use-authorization-determination mechanism that there is no authorization to use said computer;

said use-authorization-determination mechanism is activated before said attribute information-acquisition mechanism and said invalid-data-determination mechanism; and

when it is determined by said use-authorization-determination mechanism that there is no authorization to use said computer, at least one of the following; said attribute-information-acquisition mechanism or said invalid-data-determination mechanism does not execute.

25. (previously presented) The invalidity-monitoring system of claim 23 further comprising:

a profile-store for storing log data related to said input/output data as profiles for each user; and an unusual-operation-determination mechanism for referencing said profile-store and comparing input/output data that was acquired by said data-acquisition mechanism with the normal operation trend of said user to determine whether operation is unusual;

wherein said stoppage mechanism also stops an operation executed by said input/output data when it is determined by said unusual-operation-determination mechanism that operation is unusual.

26. (previously presented) The invalidity-monitoring system of claim 23, wherein said stoppage mechanism executes a process of interrupting a session when said data-acquisition mechanism acquired said input/output data from a network.

27. (previously presented) The invalidity-monitoring system of claim 23, wherein said stoppage mechanism stops a process executed by a driver when said data-acquisition mechanism acquired said input/output data from an externally connected bus.

28. (previously presented) An invalidity-monitoring system for monitoring invalid data, which

causes a computer to execute an invalid operation, the system comprising:

a computer having a connection to a network or to an external device;

a data-acquisition mechanism for acquiring input/output data that is input or output over the network that is connected to said computer, or over an externally connected bus that connects said computer with the external device;

an ID-information-identification mechanism for identifying ID information from said input/output data for identifying a user;

a user-information-store for storing attribute information for all users having authorization to use said computer;

an attribute-information-acquisition mechanism for acquiring at least part of the attribute data corresponding to said ID information from said user-information-store;

a determination-rule-storage mechanism for storing rules for determining whether said input/output data is invalid data;

an invalid-data-determination mechanism for referencing said determination-rule-storage mechanism, and determining whether said input/output data is invalid data; and

a notification mechanism for notifying a terminal being operated by said user or administrator that an operation being executed by said input/output data is an invalid operation when it is determined by said invalid-data-determination mechanism that said input/output data is invalid data;

wherein

said determination-rule-storage mechanism stores determination rules that correspond to user attributes; and

said invalid-data-determination mechanism references said determination rules that correspond to attribute information acquired by said attribute-information-acquisition mechanism to determine whether said input/output data is invalid.